

# Exhibit 10

**UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF WISCONSIN**

AUTHENTICOM, INC.,

*Plaintiffs,*

Case No. 17-cv-318-JDP

v.

CDK GLOBAL, LLC and THE REYNOLDS AND  
REYNOLDS COMPANY,

*Defendants.*

**REPLY DECLARATION OF STEVE COTTRELL**

I, Steve Cottrell, declare as follows:

1. On May 18, 2017, I submitted a declaration in this matter. I have reviewed many of the statements made by Defendants CDK Global, LLC (“CDK”) and The Reynolds & Reynolds Company (“Reynolds”) and others who have submitted declarations on their behalf. I have prepared this reply declaration to respond to some of those statements.

**A. Authenticom Accesses Only Data Controlled By The Dealership**

2. I understand Defendants have stated that allowing Authenticom, Inc. (“Authenticom”) to access dealers’ Dealer Management Systems (“DMS”) data would create security risks because that data includes social security numbers, credit card information, and intellectual property that belongs to third parties other than the dealers.

3. Authenticom accesses data in the Defendants’ DMS through reporting functions that Defendants make available to dealers. Authenticom runs these reports with the permission of the dealers and using login credentials supplied by the dealers. These reports retrieve data from five directories: sales, service, inventory, customers, and parts.

4. Authenticom translates this data into the following seven datasets: sales, service, service appointments, open repair orders, parts, inventory, and special order parts.

5. The data in the sales dataset consists of data relating to the sale of a vehicle, such as vehicle specific data, trade details, customer data, and financing data.

6. The data in the service dataset consists of data relating to repair orders, such as vehicle specific information, warranty information, parts information related to a service order, and customer and appointment information.

7. The data in the service appointments dataset consists of data relating to a scheduled repair order, including customer information and the services requested.

8. The data in the open repair order dataset consists of data relating to open repair orders, including vehicle specific data, warranty details, parts data, and customer data.

9. The data in the parts inventory dataset consists of parts that are in-stock at a dealership or on order.

10. The data in the inventory dataset consists of data relating to a vehicle on the dealership lot, or in transit to the dealer. This includes new and used vehicles and wholesale units.

11. The data in the special order parts dataset consists of parts on order.

12. The data in each of the five DMS directories is controlled by the dealers. None of the data in these directories belongs to Defendants. And none of the data in these directories is intellectual property of third parties or Defendants.

13. As a matter of practice, Authenticom requests access from the dealers to retrieve data from the five aforementioned directories. Authenticom does not access any data beyond

those five directories unless specifically directed to do so by a dealer. Authenticom is thus limited to accessing data in the DMS that is controlled by the dealers.

14. The DealerVault application then gives the dealer complete and total control over the specific data elements delivered to their vendors.

15. Authenticom does not have access to social security numbers on Defendants' DMS. The reporting functions of the DMS do not return social security numbers.

16. Social security numbers can only be viewed by users with special permissions. Such users are able to use software from the DMS provider to view or edit the social security numbers on their computer screens only. There is no export function available. Authenticom neither seeks nor is granted such permissions.

17. Authenticom does not have access to credit card information. My understanding is that credit card information is not stored on either of Defendants' DMS. If credit card information were stored on their DMS, Authenticom has no means of accessing that information.

18. Authenticom also does not have access to the dealers' financial statements, payroll records, or any other data outside of the five directories previously mentioned.

## B. Authenticom Has Strong Security Practices

19. I understand that Defendants have raised concerns about Authenticom's security practices, including the means by which it obtains login credentials from dealerships, whether it has any relevant security certifications, and the extent of Authenticom's oversight of vendors.

20. Authenticom's policy is to receive a dealer's login credentials via a secure web form. The secure web form utilizes industry standard secure socket layer ("SSL") encryption so that the login credentials cannot be intercepted by third parties.

21. In some instances, Authenticom contacts a dealer by phone to receive login credentials, and the credentials are provided over the phone.

22. Where a dealer prefers to send login credentials by email, Authenticom typically directs the dealer to provide the username and password in separate emails so that interception of either email would not disclose the full login credentials.

23. I have become aware of instances in which Authenticom employees have stated that login credentials could be sent via email without specifying that the username and password should be sent in separate emails. It has been – and continues to be – Authenticom’s policy that login credentials should be sent to Authenticom via secure web form, and, if a dealer prefers to send login credentials via email, that the username and password be sent to Authenticom in separate emails.

24. Authenticom uses Microsoft Azure cloud services as the technology infrastructure hub for its DealerVault data integration services. Authenticom stores the data that it receives from Defendants’ DMS on Microsoft Azure and then sends that data to the vendors directly from Microsoft Azure.

25. Microsoft Azure is an enterprise-grade cloud computing platform. According to Microsoft, 90% of Fortune 500 companies use Azure. Microsoft Azure uses industry-standard SSL or VPNs to secure data to and from Azure. The dealerships’ data is encrypted using AES-256 encryption while the data is stored at Microsoft Azure. Microsoft Azure also provides continual threat monitoring for potential intrusions and outbound threats, including penetration testing and denial-of-service attacks, to protect the dealerships’ data.

26. For the connection between a dealership's network (where DMS data is retrieved) and Authenticom's data center, Authenticom uses either a secure VPN connection, an industry-standard secure shell (OpenSSH), or a secure file transfer protocol ("SFTP").

27. Authenticom has Microsoft top-level gold certifications in Application Development and Cloud Platforms. These certificates require Authenticom's employees to pass rigorous exams.

28. Authenticom has long been a leader in advocating for better security practices in the automotive industry. Authenticom representatives have met repeatedly with National Auto Dealers Association ("NADA") executives (including its CEO, CTO, CFO, and chief counsel). Authenticom often speaks on data security issues at automotive industry conferences, state dealer association meetings, and virtually anywhere a group of dealers or vendors are gathering for an organized event. Moreover, Authenticom created DealerVault to provide dealers with greater control over the security of their data. At its core, DealerVault was created consistent with the guidance from NADA. Authenticom has also sent NADA's guidance publications regarding data security to thousands of dealerships.

29. Even though Reynolds claims to have concerns regarding Authenticom's security practices, Reynolds continues to allow Authenticom to offer data integration services to one of the largest dealership groups, Penske Automotive Group. My understanding is that Penske Automotive Group is the largest customer of Reynolds's DMS.

30. At the request of Penske Automotive Group, Reynolds has agreed not to block login credentials used by Authenticom to offer data integration services (so-called "whitelisting"). Authenticom offers data integration services to Penske Automotive Group using

the same techniques that Authenticom uses with other dealers (and which Reynolds claims are not secure).

31. Similarly, at automobile manufacturers' request, Reynolds agreed to whitelist login credentials used by Authenticom to offer integration services to Jaguar and BMW dealerships in order to complete customer satisfaction surveys. Authenticom offered data integration services to these Jaguar and BMW dealerships using the same techniques that Authenticom uses with other dealers (and which Reynolds claims are not secure).

32. Finally, Reynolds continues to use Authenticom to pull data for certain of its applications from both Reynolds DMS customers and CDK DMS customers even still today.

### C. Authenticom Does Not Degrade DMS Performance

33. I understand that Defendants have claimed Authenticom's data integration services can "overload" or "degrade" the performance of Defendants' DMS.

34. Authenticom's data integration services impose minimal burden on Defendants' DMS. Authenticom employs two types of queries: a bulk-data query that is run only during non-business hours and smaller queries that may be updated several times throughout the day.

35. Authenticom schedules the bulk-data query for a dealership to typically run when the dealership is closed and no one else is on the system. This query provides a daily refresh of all of the datasets that are needed by the dealership's vendors.

36. These bulk-data queries do not utilize significant DMS resources. These queries are performed while the dealership is closed, are typically completed in 8-20 minutes, and result in the transfer of approximately 5 MB of data – roughly the same size as an photo image taken with a mobile phone.

37. The queries take several minutes to complete only because Authenticom's software interacts with the DMS in sequential steps. That is, the software requests a certain set of data; the data is displayed on the screen; the software captures the data; and then the next request is sent and so on. During much of this process, there is no load imposed on the DMS by Authenticom. This process is similar to buying an airline ticket online. The process may take ten minutes because information needs to be entered on several screens; but the airline's servers are not occupied for the full ten minutes.

38. Authenticom needs to run only a single bulk-data query per day to provide data integration services to the vast majority of a dealership's vendors. Authenticom delivers data from the single bulk-data query to the dealership's various vendors according to the rules established by each dealership in DealerVault. These rules control the specific data that each vendor may receive. This improves DMS performance by eliminating the need for each vendor to run duplicative queries every day.

39. Approximately 100 of Authenticom's more than 11,000 dealership customers use vendors that need DMS data updated more frequently than the daily refreshes provided by the bulk-data queries. For these dealerships, Authenticom uses smaller queries throughout the business day. These queries typically request information pertaining to open repair orders, inventory, and service appointments.

40. These light queries utilize even less DMS resources than the bulk-data queries. These queries typically take one to five minutes to complete (during which other access to the DMS is still possible) and result in the transfer of roughly 1 MB of data.

41. Regardless of the type of query at issue, Authenticom does not run multiple queries at the same time. Authenticom requests that the queries run sequentially – *i.e.*, the

present query must end before the next may start. In this way, Authenticom mimics a dealership employee who manually runs one query after another. This provides additional assurance that Authenticom is not overly taxing the DMS.

42. I am aware of only a single instance in which Authenticom's data integration services may have impaired the performance of a DMS. Approximately 7-8 years ago, I received a call from Reynolds's Vice President of OEM Relations and Data Services Robert Schaefer. He notified me of a malfunctioning system query and asked whether this could be an Authenticom query. I directed my team to investigate the issue; we found that the query did belong to Authenticom; and we corrected the problem the same day we were notified of it.

43. Except for that isolated instance, I am unaware of any other instance in which Defendants have notified Authenticom directly about degraded DMS performance. Given Authenticom's processes, it is extremely unlikely that Authenticom could ever cause such problems.

#### **D. Authenticom Does Not Corrupt DMS Data**

44. I understand that Defendants have raised a concern that Authenticom may corrupt data in the process of "pushing" updated data to the DMS.

45. Nearly all of Authenticom's business – including its DealerVault product – does not "push" data to the DMS but rather only reads data from the DMS. When reading data from the DMS, Authenticom uses standard reporting functions developed by Defendants for their dealership customers. Since this is a read-only, export-only function, I am unaware of any way in which these reporting functions – which are Defendants' own software – could cause data corruption.

46. The only portion of Authenticom's current business that "pushes" data to the DMS is a service that Authenticom provides to cleanse the dealership's customer information stored in the DMS. By way of example, this data-cleansing service will correct errors in a customer's phone number, address, and other such information.

47. Because Authenticom only modifies individual customer records, any errors that Authenticom could introduce would be isolated to the records being modified and would not affect the DMS generally.

48. There is also little risk of errors where Authenticom "pushes" data to the DMS. Authenticom employs stringent quality control that compares the DMS data prior to any "push" operation to the DMS data after the "push" operation to ensure that the changes to the DMS data match the intended changes.

49. In Authenticom's experience, this service introduces extremely few errors. For example, Authenticom provided the data-cleansing service to Sonic Automotive, Inc., a publicly-traded dealer group with over 100 dealerships. Authenticom cleansed over nine million customer records for Sonic every month for over three years. During this period, there were less than ten errors, all easily corrected.

50. I understand that Defendants' expert Mr. Eric Rosenbach states in Paragraph 177 of his report that "emails from Authenticom to dealers explicitly request that dealers provide permission for them to update, delete and edit data. Thus, it appears that Authenticom attempts to actively change the data resident in the DMS system which introduces significant operational risk."

51. For that statement, Mr. Rosenbach relies upon a document titled "R&R Dynamic Reporting Access Set Up." Dynamic Reporting is a tool offered by Reynolds that allows dealers

to manually run reports and download the resulting data. This document explains to dealers how to set up Dynamic Reporting so that Authenticom can run those reports and perform services on behalf of dealerships using those reports. Page six of the document directs dealerships to grant Authenticom permission to “Add Report,” “Delete Report,” “Edit Report when Owner” (meaning only those reports created for Authenticom) and “Run Report.”

52. The permissions described in this document allow Authenticom only to create, delete, and edit *reports* that pull from the specific directories to which the dealer has granted Authenticom permission. The specific permissions referenced in this document allow Authenticom to generate, delete, and change the reports. These permissions do not give Authenticom any ability to create, delete, or edit *data* in the DMS, or any directory access not granted by the dealer.

#### **E. Authenticom Pricing**

53. As I explained in my initial declaration, Authenticom charges, on average, \$30 to \$40 per month for data-pulling services. I understand that Defendants have cited to one vendor contract from 2013 and claims it is “evidence of Authenticom charging higher amounts.” *See* Defs. RSOF ¶¶ 68, 71; Defs. Ex. 64.

54. The contract reflected in Defs. Ex. 64 was between Authenticom and a vendor called XtreamService, which is now a wholly owned subsidiary of Reynolds. Since July 2013, Authenticom has provided XtreamService with data-pulling services at two dealerships.

55. For the XtreamService contract, at the customer’s request, Authenticom waived its standard up-front \$2,500 deposit and instead initially charged a slightly higher than average monthly rate (\$70). This was before Authenticom introduced standardized pricing through

DealerVault. Since June 2014, Authenticom has charged Reynolds (now the parent company of XtreamService) a rate of \$45 per month at two dealerships (for a total of \$90 per month).

56. When it was first signed in 2013, the XtreamService contract also included a “one-time fee” of \$200 per rooftop (or \$400 total for the two serviced dealerships). Authenticom no longer charges a per-dealership setup fee; it only charges one-time fees for vendors that need Authenticom to pull historical data going back further than 90 days. The one-time historical data fee is \$50 per year of data with a maximum of \$200 per rooftop.

57. I also note that the goodwill generated by Authenticom in providing data integration services results in many of our vendor customers also purchasing our data hygiene services.

#### **F. Reynolds’ Use of Authenticom for Integration Services**

58. Reynolds has long used Authenticom to pull data from dealers using various DMS systems, including the Reynolds DMS, CDK DMS, and many others. Authenticom uses the standard process to pull data from those dealers, namely, dealer-authorized user names and passwords, which Reynolds oftentimes provides to us. I understand that Mr. Robert Schaefer of Reynolds stated in his declaration that he is “not aware of Reynolds currently using Authenticom to pull data from any Reynolds dealerships for us in Reynolds’ own applications.” Schaefer Decl. ¶ 104. Mr. Schaefer is incorrect about Reynolds’ use of Authenticom for data integration services.

59. A spreadsheet with backup workbooks will be filed with Authenticom’s reply papers. That spreadsheet lists the Reynolds applications for which Authenticom provides data integration services. The spreadsheet also identifies those *Reynolds dealers* and *CDK dealers* from which Authenticom pulls data for Reynolds’ applications. The spreadsheet likewise

provides the extensive historical record of Authenticom providing data integration services for Reynolds' own applications from Reynolds dealers (and those of CDK).

60. The “Summary” tab lists the six Reynolds applications for which Authenticom has provided integration services: (1) AIMData, Inc.; (2) IMN Inc.; (3) Integrated Document Solutions; (4) Naked Lime Reputation Management; (5) Reynolds Remindertrax; and (6) Showroom Magnet. Authenticom is still providing data integration services for all of them except IMN, Inc.

61. In the “Summary tab,” listed below each application are the numbers of CDK dealers (“ADP Web Alliance” and “CDK”) and Reynolds dealers (“R&R”) from which Authenticom pulls data for Reynolds. Each column is broken down by quarter by year (2008 – 2017), and the numbers listed in each row are the number of CDK or Reynolds dealers from which Authenticom pulled or pulls data for the Reynolds application. The totals for each quarter are in the last row.

62. Using “Showroom Magnet” as an example, Authenticom still pulls from 3 Reynolds dealers as of today.

63. I also note the effect of the CDK and Reynolds February 2015 written agreement on Reynolds’ use of Authenticom for integration services. After Reynolds and CDK entered into that agreement, Reynolds significantly decreased its use of Authenticom, presumably because now Reynolds was getting the data from CDK’s integration service. Using “Integrated Document Solutions” as an example, Authenticom pulled data from 204 CDK dealers in October 2015. That number dropped to 14 CDK dealers at the end of 2016, and is currently at 7 dealers.

64. As for totals, the numbers show how extensively Reynolds relied (and relies) on Authenticom for integration services. For example, Authenticom pulled data from at least 358

CDK and Reynolds dealers in 2014; 320 CDK and Reynolds dealers in 2015; 78 CDK and Reynolds dealers in 2016; and 33 CDK and Reynolds dealers today.

65. I've always thought that Reynolds' extensive historical use of Authenticom for integration services – and existing use today – shows that Reynolds' arguments with respect to "security" are not that credible, especially in light of my company's unblemished security record.

Executed in Washington, D.C., on June 22, 2017.

By:



Steve Cottrell